UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/658,561	09/08/2003	Jyshyang Chen	O2MICRO 02.20	3263

79708 7590 09/18/2008

O2Micro/GTPP
55 South Commercial Street
Manchester, NH 03101

EXAMINER	
PATEL, NIRAV B	

ART UNIT	PAPER NUMBER
2135	

NOTIFICATION DATE	DELIVERY MODE
09/18/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

drobertson@gtpp.com
docketing@gtpp.com

Office Action Summary	Application No.	Applicant(s)	
	10/658,561	CHEN, JYSHYANG	
	Examiner	Art Unit	
	NIRAV PATEL	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 June 2008 (Amendment)*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8-13,15 and 16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6, 8-13, 15, 16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on June 03, 2008 has been entered. Claims 1-6, 8-13, 15, 16 are pending.

2. Examiner has acknowledged the applicant statement that claim 1 (similar claim 9) includes **hardware** i.e. an integrated firewall/VPN chipset/circuit. Therefore, the 35 U.S.C. 101 rejection is withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-3, 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vairavan (US Pub. No. 2002/0083344) in view of Hui et al (US Pub. No. 2004/0010712) in view of Canion et al (US Patent No. 2002/0108059) in view of Foschiano et al (US Pub. No. 2004/0022253) and in view of Yang et al (US Patent No. 7,003,118).

As per claim 1, Vairavan discloses:

at least one wide area network (WAN); at least one local area network (LAN) [Fig. 1, paragraph 0047, 0048]; and an integrated firewall/VPN chipset configured to send and

receive data packets between said WAN and said LAN [Fig. 1, component 110]. Further, Vairavan teaches filtering techniques within different firewall layers [paragraph 0086, 0087 – i.e. a firewall comprising multiple layers], a first layer including a header match packet filtering engine configured to provide pattern matching in selected headers of data, a second layer including a content match packet filtering engine configured to analyze the scope of at least one data packet [paragraph 0074-0079, 0086, 0088, 0137 lines 1-3].

Hui teaches a firewall which provides packet filtering function along with application proxy function (i.e. a third layer), a third layer including at lest one application proxy configured to provide additional pattern matching [paragraph 0220]. Further, Hui teaches a listening table which stores a TCP/UDP connection setup in a look-up-table [paragraph 0070, 0149] and to forward the setup progress to said CPU for tracking [paragraph 0070, 0084, 0090, 0105].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Hui with Vairavan, since one would have been motivated to improve speed/security for firewall and speed for VPN [Hui, paragraph 0009].

Canion teaches a fourth layer including a session match engine configured to store a TCP/UDP connection setup in a look-up-table and to forward the setup progress to said CPU for tracking [paragraph 0067, 0068, 0072].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Canion with Vairavan and Hui, since one would

have been motivated to examine the packet for security violation to distinguish real requests from attack based requests [Canion, paragraph 0009].

Foschiano teaches hardware engine to provide pre-analysis processing to reduce the workload of a central processing unit (CPU) [paragraph 0060, 0042].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Foschiano with Vairavan, Hui and Canion, since one would have been motivated to prevent overload of the inspection engine [Foschiano, paragraph 0042].

Further, Vairavan discloses:

a VPN configured to provide security functions for data between said LAN and said WAN, wherein said security functions are selected from the group consisting of encryption, decryption, encapsulation, and decapsulation of said data packets [paragraph 0109, 0112]; an interface configured to determined if said data packets are plain text or cipher text, said interface further configured to forward a preselected number of bytes to said firewall if said data packet are plain text, said interface further configured to forwarded said data packets to said VPN if said data packets are cipher text [Fig. 6A, 7, 8, paragraph 0132]. Further, Vairavan teaches a VPN processor configured to decrypt and decapsulate said at least one data packet, said VPN further includes an inbound security database having database of tunnels configured to provide VPN processor with tunnel information used to decrypt and decapsulate said at least one data packet, said VPN further including protocol instructions having macrocodes configured to instruct said VPN processor to decrypt and decapsulate said at least one

data packet according to a user-defined security procedure [paragraph 0080-0085, 0091-0101].

Yang teaches: the VPN including a VPN packet buffer configured to receive at least one of said data packets and to forward said at least one data packet to an inbound VPN processor to decrypt and decapsulate said at least one data packet, said VPN further including an inbound security database having a database of tunnels configured to provide VPN processor with tunnel information used to decrypt and decapsulate said at least one data packet [Fig. 5, 6, col. 8 lines 8-67, col. 9 lines 1-18].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Yang with Vairavan, Hui, Canion and Foschiano, since one would have been motivated to increase the speed for the network security operation related to IPSEC and Authentication Headers [Yang, col. 1 lines 19-21].

As per claim 2, the rejection of claim 1 is incorporated and Vairavan discloses:

said chipset further comprises a router adapted to route data between said WAN and said LAN [Fig. 1, 2, paragraph 0058, 0122, 0139 lines 1-4].

As per claim 3, the rejection of claim 1 is incorporated and Vairavan teaches said firewall is configured to provide static and/or dynamic data packet filtering (i.e. based on filtering rules/policy) [paragraph 0074].

As per claim 9, it encompasses limitations that are similar to limitations of claims 1 and 2. Thus, it is rejected with the same rationale applied against claims 1 and 2 above.

As per claim 10, the rejection of claim 9 is incorporated and it encompasses limitations that are similar to limitations of claim 3. Thus, it is rejected for the same reason set forth in the rejection of claim 3 above.

4. Claims 4 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vairavan (US Pub. No. 2002/0083344) in view of Hui et al (US Pub. No. 2004/0010712) in view of Canion et al (US Patent No. 2002/0108059) in view of Foschiano et al (US Pub. No. 2004/0022253) and in view of Yang et al (US Patent No. 7,003,118) and in view of Lee (US Patent No. 7,047,561).

As per claim 4, the rejection of claim 1 is incorporated and Lee teaches said header match packet filtering engine is configured to provide pattern matching in selected headers of said data and their combination from L2, L3 and L4 headers [Fig. 5].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Lee with Vairavan, Hui, Canion, Foschiano and Yang, since one would have been motivated to provide the necessary speed/security for real-time Internet applications [Lee, col. 2 lines 15-17].

As per claim 11, the rejection of claim 10 is incorporated and it encompasses limitations that are similar to limitations of claim 4. Thus, it is rejected for the same reason set forth in the rejection of claim 4 above.

5. Claims 5, 6, 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vairavan (US Pub. No. 2002/0083344) in view of Hui et al (US Pub. No. 2004/0010712) in view of Canion et al (US Patent No. 2002/0108059) in view of Foschiano et al (US Pub. No. 2004/0022253) in view of Yang et al (US Patent No. 7,003,118) and in view of Krishna et al (US Patent No. 6,477,646).

As per claim 5, the rejection of claim 1 is incorporated and Vairavan discloses the chipset further configured to analyze access control functions [0086, 0132].
Krishna teaches a security chip to incorporate both encryption and authentication functionality in a signal chip [Fig. 2, 4]. Further, Kim teaches processing the packet based on preselected bytes of the data packet [col. 3 lines 64-67, col. 4 lines 1-2, col. 5 lines 38-50].
Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Krishna with Vairavan, Hui, Canion, Foschiano and Yang, since one would have been motivated to improve the performance improvement [Krishna, col. 2 lines 26-27].

As per claim 6, the rejection of claim 5 is incorporated and Krishna teaches:

said preselected bytes comprise the first 144 bytes of said data packet [col. 4 lines 1-2, col. 6 lines 28-32].

As per claim 12, the rejection of claim 9 is incorporated and it encompasses limitations that are similar to limitations of claim 5. Thus, it is rejected for the same reason set forth in the rejection of claim 5 above.

As per claim 13, the rejection of claim 12 is incorporated and it encompasses limitations that are similar to limitations of claim 6. Thus, it is rejected for the same reason set forth in the rejection of claim 6 above.

6. Claims 8, 15 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vairavan (US Pub. No. 2002/0083344) in view of Hui et al (US Pub. No. 2004/0010712) in view of Canion et al (US Patent No. 2002/0108059) in view of Foschiano et al (US Pub. No. 2004/0022253) and in view of Yang et al (US Patent No. 7,003,118) and in view of Osborne et al (US Patent No. 6,687833).

As per claim 16, Vairavan discloses:

filtering techniques within different firewall layers [paragraph 0086, 0087 – i.e. a firewall comprising multiple layers], a first layer including a header match packet filtering engine, a second layer including a content match packet filtering engine configured to analyze the scope of at least one data packet [paragraph 0074, 0086, 0088, 0137 lines 1-3].

Further, Vairavan discloses:

a VPN configured to provide security functions for data between said LAN and said WAN, wherein said security functions are selected from the group consisting of encryption, decryption, encapsulation, and decapsulation of said data packets [paragraph 0109, 0112]; an interface configured to determined if said data packets are plain text or cipher text, said interface further configured to forward a preselected number of bytes to said firewall if said data packet are plain text, said interface further configured to forwarded said data packets to said VPN if said data packets are cipher text [Fig. 6A, 7, 8, paragraph 0132]. Further, Vairavan teaches a VPN processor configured to decrypt and decapsulate said at least one data packet, said VPN further includes an inbound security database having database of tunnels configured to provide VPN processor with tunnel information used to decrypt and decapsulate said at least one data packet, said VPN further including protocol instructions having macrocodes configured to instruct said VPN processor to decrypt and decapsulate said at least one data packet according to a user-defined security procedure [paragraph 0080-0085, 0091-0101].

Hui teaches a firewall which provides packet filtering function along with application proxy function (i.e. a third layer), a third layer including at lest one application proxy configured to provide additional pattern matching [paragraph 0220]. Further, Hui teaches a listening table which stores a TCP/UDP connection setup [paragraph 0070, 0149] and to forward the setup progress to a central processing unit (CPU) for tracking [paragraph 0070, 0084, 0090, 105].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Hui with Vairavan, since one would have been motivated to improve speed/security for firewall and speed for VPN [Hui, paragraph 0009].

Canion teaches a fourth layer including a session match engine configured to store a TCP/UDP connection setup and to forward the setup progress to a central processing unit (CPU) for tracking [paragraph 0067, 0068, 0072].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Canion with Vairavan and Hui, since one would have been motivated to examine the packet for security violation to distinguish real requests from attack based requests [Canion, paragraph 0009].

Foschiano teaches hardware engine to provide pre-analysis processing to reduce the workload of a central processing unit (CPU) [paragraph 0060, 0042].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Foschiano with Vairavan, Hui and Canion, since one would have been motivated to prevent overload of the inspection engine [Foschiano, paragraph 0042].

Yang teaches: the VPN including a VPN packet buffer configured to receive at least one of said data packets and to forward said at least one data packet to an inbound VPN processor to decrypt and decapsulate said at least one data packet, said VPN further including an inbound security database having a database of tunnels configured to

provide VPN processor with tunnel information used to decrypt and decapsulate said at least one data packet [Fig. 5, 6, col. 8 lines 8-67, col. 9 lines 1-18].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Yang with Vairavan, Hui, Canion and Foschiano, since one would have been motivated to increase the speed for the network security operation related to IPSEC and Authentication Headers [Yang, col. 1 lines 19-21].

Osborne teaches: defining one or more access control protocols [Fig. 3, col. 5 lines 27-65]; receiving a data packet [Fig. 2]; selecting a certain number of bytes of said data packet; processing said selected bytes using said access control protocols [Fig. 8, 9 col. 6 lines 60-67, col. 7 lines 6-21].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Osborne with Vairavan, Hui, Canion and Yang, since one would have been motivated to provide network security system capable of diverting and tracking potential attacks [Osborne, col. 2 lines 12-13].

As per claim 8, the rejection of claim 1 is incorporated and Vairavan teaches said firewall further includes access control modules [Fig. 4, 5].

Osborne teaches access control function comprising user-defined access control protocols [Fig. 2, 3].

As per claim 15, the rejection of claim 9 is incorporated and it encompasses limitations that are similar to limitations of claim 8. Thus, it is rejected for the same reason set forth in the rejection of claim 8 above.

Response to Argument

7. Regarding to the 35 USC § 101 rejection, Examiner has acknowledged the applicant statement that claim 1 (similar claim 9) includes **hardware** i.e. an integrated firewall/VPN chipset/circuit. Therefore, the 35 U.S.C. 101 rejection is withdrawn.

Applicant's arguments filed April 21, 2008 have been fully considered but they (arguments related to 35 USC 103 rejection) are not persuasive.

Regarding to applicant argument to claim 1, Examiner maintains, since Vairavan's invention relates to the field of enterprise networking and inter/intra-networking interfacing between various types of networks. The inter/intra-networking device comprises a plurality of access device cards, a packet processor, a security processor, a system processor and a switching fabric. The access device cards support various access devices that interface with the inter/intra-networking device. The packet processor performs various security, routing, encryption/decryption and management functions on packets received from the access device cards. The security processor operates both independently and in cooperation with the packet processor in the creation and maintenance of secured virtual private network connections within

attached networks. The security processor decrypts and encrypts packet according to a protocol defined standard architecture. The system processor configures each of the components within the inter/intra-networking device to function properly as well as coordinates and supervises each these components. The system processor is coupled to each component via a plurality of control lines so that management data communicates quickly and efficiently. The system processor coordinates with the packet processor to perform various security functions and firewall intrusion detection operations. The system processor also logs events that occur both within the inter/intra networking device and on the attached networks. The switching fabric is coupled to the packet processor and system processor. The switching fabric includes numerous network ports that is connected to various different local area network and/or private networks or connect to a single network. The switching fabric comprises multiple routing and switching tables that allow the switching fabric to transmit packets to an appropriate destination on an attached network. Fig. 2 shows a block diagram of the inter/intra networking device. The packet processor performs multiple packet analyses and functions upon receipt of a packet from the packet bus. The packet processor extracts and analyzes relevant management data included within packets. **This management data is used to create and maintain management tables such as policy, network configuration and service tables. The packet processor performs various functions to create, maintain and control virtual private networks ("VPNs") with the enterprise**. The packet processor also provides various security functions (e.g. firewalls, tables of security associations and associated information, IPSec processing

and database, anti-virus program, and port protection and blocking standards) that protect the integrity of the inter/intra networking device, the enterprise and attached devices. As shown in Fig. 3, the packet processor comprises a security policy database, which includes a standard for specifying packet filtering rules based on information found within a header of a packet. A firewall module contains multiple firewalls, which access the security policy database to retrieve a particular security standard or packet analysis algorithm. **The firewall module analyzes, isolates and discards packets according to security standards and filtering techniques within different firewall layers [paragraph 0086]**. Various filtering algorithms are used to characterize packets received by the firewall module (content and/or state filtering). The firewall module controls access to various functionalities and site within a VPN. A VPN policy and table maintains the procedures for authenticating a communicating peer, creation and management of security association, key generation techniques, and threat mitigation. These functions are necessary to establish and maintain secure communications in an Internet environment. The packet processor identifies a packet type corresponding to the received packet (VPN or wireless packet...etc.), and then firewall-filtering rules are applied to specific header field value within the packet. For VPN packet, VPN functions are performed to create or maintain a secure connection between the source and destination device. Therefore, Vairavan teaches the VPN/Firewall mechanism. Further, in analogous art, Hui discloses a method, device and system relating to network firewalls and VPN gateways for controlling and securing access to networks. An integrated VPN/Firewall system [Fig. 3] comprises at least one policy engine, switch

module, a cryptographic engine module and at least one flow engine module. The policy engine module performs pattern matching for content filtering, virus scanning and for scanning for keywords as an application layer proxy. The policy engine module also use the TCP protocol offload capability of the flow engine modules for application layer proxy applications and for communicating with outside servers for authentication/authorization content filtering and virus scanning. The flow engine module is used to speed up repetitive functions and as a general CPU to assist in orchestrating the hardware functions. Further the policy engine inserts a listening table entry for setting up a connection. Therefore, **Hui teaches the integrated VPN/Firewall device that provides further pattern matching and flow control mechanism to improve the speed and security of the device**. Further, Canion teaches storing the connection setup in a look-up table, which is used for identification of the location in the transport processing engine [paragraph 0072, 0068]. Therefore, it provides tracking mechanism as claimed. Foschiano teaches inspecting the packet to prevent erroneous and/or unauthorized bindings from being given effect. If the packets are illegal, eight due to malicious or mistaken actions, the illegal packet is dropped. Further, rate limiting is achieved by dropping the packet prior to analysis by shutting down a port transmitting large volumes of such packets or other appropriate response. This prevents packet storms, and the overload of the inspection engine analyzing such packets. Further, Foschiano teaches forwarding engine proceeds with pre-inspection analysis of the packet. Therefore, Foschiano's invention provides pre-analysis processing to reduce the workload of the engine. In this case the combination of Vairavan, Hui, Canion,

Foschiano and Yang teaches the claim subject matter. In fact, Vairavan, Hui, Canion, Foschiano and Yang do not need to disclose anything over and above the invention as claimed in order to render it unpatentable or anticipate. A recitation of the intended use of the claimed invention must result in structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claimed limitations.

For the above reasons, it is believed that the rejections should be sustained.

Conclusion

8. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

NBP
9/8/08

/KimYen Vu/

Supervisory Patent Examiner, Art Unit 2135